Network Security Situation Prediction in Software Defined Networking Data Plane

Mingren Sheng
School of Computer Science and Technology, Research Institute of CyberSpace Security
Harbin Institute of Technology
Weihai, China
e-mail: shengmr911@qq.com

Hongri Liu
School of Computer Science and Technology, Research Institute of CyberSpace Security
Harbin Institute of Technology
Weihai, China
e-mail: lhr_5687@163.com

Xu Yang
School of Computer Science and Technology, Research Institute of CyberSpace Security
Harbin Institute of Technology
Weihai, China
e-mail: yangxu7991@foxmail.com

Wei Wang
School of Computer Science and Technology, Research Institute of CyberSpace Security
Harbin Institute of Technology
Weihai, China
e-mail: wwhit@hit.edu.cn

Junheng Huang
School of Computer Science and Technology, Research Institute of CyberSpace Security
Harbin Institute of Technology
Weihai, China
e-mail: hithjh@163.com

Bailing Wang*
School of Computer Science and Technology, Research Institute of CyberSpace Security
Harbin Institute of Technology
Weihai, China
e-mail: wbl@hit.edu.cn

***Abstract*—Software-Defined Networking (SDN) simplifies network management by separating the control plane from the data forwarding plane. However, the plane separation technology introduces many new loopholes in the SDN data plane. In order to facilitate taking proactive measures to reduce the damage degree of network security events, this paper proposes a security situation prediction method based on particle swarm optimization algorithm and long-short-term memory neural network for network security events on the SDN data plane. According to the statistical information of the security incident, the analytic hierarchy process is used to calculate the SDN data plane security situation risk value. Then use the historical data of the security situation risk value to build an artificial neural network prediction model. Finally, a prediction model is used to predict the future security situation risk value. Experiments show that this method has good prediction accuracy and stability.**

Keywords—network security, software-defined network, time series classification, bidirectional long short-term memory network

I. INTRODUCTION

With the continuous expansion of the network scale in recent years, the lack of the traditional hierarchical network structure has gradually emerged. In 2009, Professor Mckeown of Stanford University proposed the concept of software-defined networking (SDN) [1]. The core feature of SDN is to separate the control logic and forwarding behavior in network forwarding as different levels, and the application plane is composed of various network services, and the forwarding is managed through the control plane. A unified and open data interface (such as OpenFlow [2]) is used to communicate between the control plane and the data plane. The control plane sends forwarding rules to the data plane switch through this interface. The switch only needs to perform forwarding according to the rules. Obviously, SDN technology effectively reduces the load of forwarding equipment, and centralized control also provides convenience for network operation and management, and also greatly improves the flexibility of the network.

Due to the layered idea of centralized control, the SDN structure itself also brings new security issues. Combined with the idea of SDN's own centralized management, security situation awareness as a globally coordinated and centralized management security monitoring method is considered to be an effective means of managing SDN security. The process of situational awareness is usually divided into situational element acquisition, situational assessment, and situational prediction. In the SDN environment, there is no mature method for assessing and predicting the security situation that affects the SDN architecture. This paper proposes a security situation prediction method based on particle swarm optimization (PSO) algorithm and long short-term memory (LSTM) neural network. This method uses the network security event information to evaluate and predict the security situation of the SDN data plane, so as to provide more targeted and valuable security intelligence for network managers and security analysts.

II. RELATED WORK

In the network security situation assessment, a parallel reduction algorithm based on attribute importance matrix is proposed to reduce the attributes of the data source data [3]. A network security situation assessment model based on a gravity search algorithm is proposed to optimize support vector machines to reduce the error between the evaluation value and the actual network security situation value [4]. A random forest-based network security situation assessment model is proposed to make the assessment more objective and accurate [5]. None of the above methods can effectively assess the situation based on the structural characteristics of the SDN environment.

In the network security situation prediction, a network attack prediction model combining extreme value theory and

978-1-7281-6521-9/20/$31.00 ©2020 IEEE

time series theory is proposed, which is effective for both long term and short term prediction [6]. An automated network attack prediction system that uses various public and personal data sources and uses capture technology is proposed to predict future network security events [7]. Data from security service providers are used to analyze the correlation between security event contexts and predict security events accordingly [8]. The above situation prediction methods are only applicable to the traditional network environment, and it is difficult to smoothly migrate to the SDN environment.

Artificial neural networks can be widely used in the research of nonlinear systems and can predict the changing laws of network traffic [9]. The neural network has a complex structure, so the training process will also have defects. During the iterative process, the optimization may be slower or fall into local extremes, resulting in lower prediction accuracy [10]. PSO algorithm applied to the optimization of the LSTM neural network can avoid the above problems [11]. The combined prediction method combines more than two methods with their respective advantages to form a new prediction model, which can show better prediction performance.

In summary, the current security situation assessment and prediction technology for SDN architecture are still at the theoretical and framework stage. Among the security incidents known to affect the SDN architecture, a large number of security incidents are caused by attacks on the switch. Therefore, the evaluation of the security situation affecting the SDN architecture needs to focus on analyzing data plane security incident information. This paper designs the security situation assessment method for the SDN data plane, and then apply the related technology of time series regression to the network security situation prediction.

III. Proposed Method and Model

A. Situation assessment model

Common network attacks in the SDN data plane are divided into the following categories:

- ARP Flood, Flood fake ARP packets trying to crack the ARP cache in controller or poison the ARP cache of other hosts.
- LLDP Flood, Flood gratuitous LLDP packets trying to poison the network topology or impact the controller topology manage function.
- DoS Attack, Flood other hosts with fake source IP addresses using TCP or UDP.
- Port Scan, Scanning hosts' open ports inside the network.
- LLDP Replay, Replay received LLDP packets trying to poison the network topology impact the controller topology manage function.

This paper uses a hierarchical model based on the frequency of network security events to solve the problem of network security situation assessment in the SDN data plane environment. This paper calculates the security situation risk value based on the possibility of different security incidents and the severity of the damaging effect, combined with the frequency of recent security incidents.

The model contains four granular statistics of network security events, with 5min, 15min, 60min, and 180min as the time period respectively. The number of a type of network security event within a certain period of time is denoted as C_{ij}, the length of the corresponding counting period is denoted as L_j, and the unit of period length is an hour. The frequency index of the occurrence of a security event is one of the parameters for calculating the risk value, which is mainly the ratio of the number of security events C_{ij} to the length of the corresponding counting period L_j in a certain period of time. When calculating the frequency, normalization is required. In (1), (2) and (3), subscript *j* represents four calculation periods, subscript *i* represents five events.

$$C = \begin{bmatrix} C_{11} & \cdots & C_{14} \\ \vdots & \ddots & \vdots \\ C_{51} & \cdots & C_{54} \end{bmatrix} \tag{1}$$

$$F_{ij}(t) = \frac{C_{ij}(t)/L_j}{\max(C_{ij}(t)/L_j)} \times R_j \times S_i \tag{2}$$

According to the length of the duration period L_j corresponding to the frequency index of the security event, different situation evaluation weights R_j are given. The weight R_j takes a value between 0 and 1. Experiments show that the shorter the sampling time, the more intense the frequency fluctuations. So a suitable sampling time should be given a larger R_j. According to the severity of security incidents, the five security incidents are divided into three categories (destroying the topology information in the controller, causing massive flow tables to be issued, and consuming link resources). The possibilities are collectively summarized as losses caused by security incidents. Different evaluation weights S_i are given to different security events, respectively. The weight S_i takes a value between 0 and 1.

$$F(t) = \sum_{\substack{1 \le i \le 5 \\ 1 \le j \le 4}} \frac{C_{ij}(t)/L_j}{\max(C_{ij}(t)/L_j)} \times R_j \times S_i \tag{3}$$

Considering that the switches in the SDN data plane are white box switches, the asset value of each switch is almost equal, so the situation assessment of the data plane can ignore the proportion of asset value. $F(t)$ is the security situation risk value of the SDN data plane at this time.

B. Situation prediction model

This paper makes improvements to the PSO algorithm [12] and proposes a Nonlinear Dynamic Particle Swarm Optimization Algorithm (NDPSO). This algorithm adjusts the parameters of the PSO algorithm nonlinearly so that the particles have constantly changed search capabilities at different times to balance the global and local search capabilities of the particles. At the same time, it also adjusts the out-of-bounds particles so that the out-of-bounds particles do not gather at the boundary to solve the problem that the PSO algorithm is prone to fall into the local extreme value, thereby improving the optimization performance of the algorithm.

The NDPSO algorithm proposed in this paper adjusts the speed and position of the particles in each iteration as follows:

$$V_{i,j}^{t+1} = \omega^t V_{i,j}^t + c_1^t r_1 \left(pbest_{i,j}^t - x_{i,j}^t\right) + c_2^t r_2 \left(gbest_j^t - x_{i,j}^t\right) \tag{4}$$

$$X_{i,j}^{t+1} = X_{i,j}^{t} + V_{i,j}^{t+1} \quad (5)$$

$$\omega^t = \omega_{\min} + (\omega_{\max} - \omega_{\min}) \times (t/t_{max} - 1)^2 \quad (6)$$

$$c_1^t = c_{1\,start} - (c_{1\,start} - c_{1\,end}) \times (\omega^t - 1)/2 \quad (7)$$

$$c_2^t = c_{2\,start} + (c_{2\,end} - c_{2\,start}) \times (\omega^t - 1)/2 \quad (8)$$

The PSO algorithm sets the inertia factor ω as a constant. The NDPSO algorithm in this paper makes the parabolic shape of ω decrease, which can make the particle search range in the early stage larger and the search granularity finer in the later stage.

The sizes of c_1 and c_2 of the PSO algorithm are constant 2. In this paper, the values of c_1 and c_2 are set as a function of the inertia factor ω, so that the learning factor is linked to the changing law of the inertia factor. Let $c_{1\,start} = c_{2\,end} = 3$, $c_{1\,end} = c_{2\,start} = 1$, so that $c_1 + c_2 = 4$, which is more in line with the setting value of the PSO algorithm similarly, the change rule is the same as the inertia factor ω. As the number of iterations increases, the self-learning ability of each particle gradually decreases, and the social learning ability gradually increases. That is, the early stage pays more attention to the individual's free development, and the later stage prefers the fine search for the optimal position of the group.

t is the current iteration number, $V_{i,j}^t$ and $x_{i,j}^t$ represents the velocity and position of the particle *i* in the *j*-th dimension at the *t*-th iteration; $pbest_{i,j}^t$ is an individual extremum, which is the historical optimal position found by particle *i*; r_1 and r_2 are random numbers between 0 and 1; $gbest_j^t$ is a global extremum, which represents the best position the particles can find; V_{max} and X_{max} are the maximum particle speed and maximum position.

When$X_{i,j}^{t+1} > X_{max}$:

$$X_{i,j}^{t+1} = rand(X_{i,j}^{t},\ X_{max}) \quad (9)$$

When$X_{i,j}^{t+1} < -X_{max}$:

$$X_{i,j}^{t+1} = -rand(X_{i,j}^{t},\ X_{max}) \quad (10)$$

The above operation can make the cross-boundary particles randomly return to the middle area between the previous position and the boundary position to continue to optimize, thereby improving the overall search ability of the particles.

LSTM can usually be used to solve time series prediction problems. The Bidirectional Long Short-Term Memory (BiLSTM) can find the law in both the positive and negative directions of the time series, so it can show a stronger effect on the processing of certain problems. This paper introduces LSTM and BiLSTM into the security situation prediction system of the SDN data plane.

Since the number of hidden layer nodes of neural networks generally does not exceed the number of input layer nodes, manually setting the number of hidden layer nodes will bring a lot of work, and may lose the optimal solution and lead to low prediction accuracy. Therefore, in this paper, the NDPSO is used to calculate the number of hidden layer nodes of LSTM and BiLSTM, so as to establish a suitable neural network prediction model.

The specific process of NDPSO algorithm to optimize the structure of LSTM or BiLSTM neural network is as follows:

1) Initialize the algorithm's parameters;

2) Initialize the LSTM or BiLSTM neural network structure;

3) Set the fitness function of the NDPSO as the loss function of the neural network. In this paper, the mean square error function is used as the fitness function.

$$fit_{MSE} = \frac{1}{n}\sum_{i=1}^{n}(\hat{y}_i - y_i)^2 \quad (11)$$

In the formula, n is the particle swarm size, and $\hat{y}_i$ and y_i are the predicted value and the true value respectively.

4) Calculate the fitness function value of each particle;

5) Update the local optimal position of each particle and the global optimal position of the particle swarm;

6) Update each particle's own speed and position;

7) If the maximum number of iterations is not reached, go to step *4)*.

IV. Simulation Results and Analysis

A. Experiment Environment

To evaluate our method, we deployed a simple network topology using the controllers of Mininet [13] and ONOS [14]. In this topology, there are two SDN switches, and each SDN switch is connected to two hosts. One of the four hosts is marked as a malicious host. All four hosts will send internal communication traffic on the network. Referring to [15], network traffic is generated using a traffic generator named D-ITG [16]. When a malicious host sends legitimate traffic, it will also send attack traffic. Attack traffic is generated with Scapy [17]. We generate 16 hours of traffic for all hosts, and malicious hosts attack during this period. The intrusion detection system is responsible for collecting security event information on the data plane. The security situation assessment module calculates the security situation risk value according to the security event information and divides this data into a training set and a test set according to the proportion of 80% and 20%. We trained four artificial neural network models, LSTM, BiLSTM, NDPSO-LSTM, and NDPSO-BiLSTM, to compare the prediction results. Then use the prediction model with the best effect to make predictions for three periods of time respectively, and analyze the prediction results.

B. Evaluation Indicators

The root mean squared error (RMSE) and the mean absolute percentage error (MAPE) are selected as the evaluation criteria. MAPE calculates the error percentage, so MAPE can also be used to calculate model prediction accuracy.

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(f_i - y_i)^2} \quad (12)$$

$$MAPE = \frac{1}{n}\sum_{i=1}^{n}\left|\frac{f_i - y_i}{y_i}\right| \quad (13)$$

Where f_i is the predicted value, y_i is the actual value of the safety situation indicator, and n is the scale of the test data.

C. Model Comparison Experiment Results

The prediction results of the four models on the risk value of the security situation in the next 2 minutes are shown in Fig. 1 and Fig. 2. The prediction error of BiLSTM model and LSTM model is larger, and the former has a smaller prediction value, while the latter has a larger prediction value. The BiLSTM and LSTM models combined with NDPSO have good prediction effects, and the predicted value of NDPSO-BiLSTM is closest to the true value, and the absolute value of the prediction error does not exceed 12%.

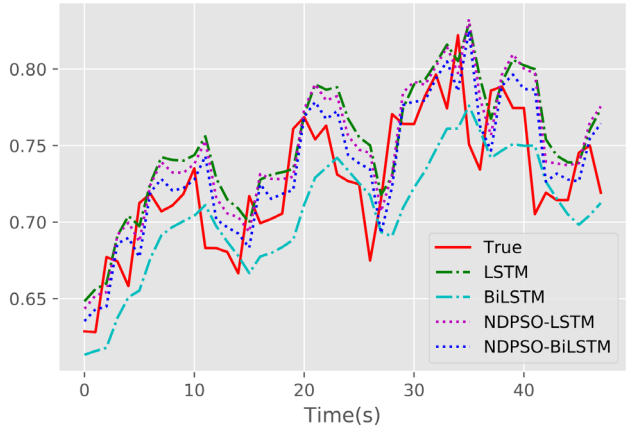

Fig. 1. Normalized data prediction result of safety situation risk value

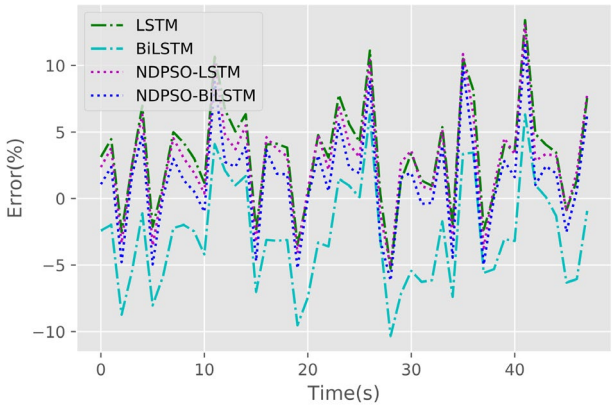

Fig. 2. Comparison of prediction errors of four models

TABLE I. EVALUATION INDEXES OF PREDICTION RESULTS

Model	RMSE	MAPE (%)
LSTM	0.009477	4.2562
NDPSO-LSTM	0.008949	4.0281
BiLSTM	0.009236	4.0835
NDPSO-BiLSTM	0.007671	3.2249

In this experiment, the prediction effect of BiLSTM model is better than that of LSTM model as shown in TABLE I. The prediction effect of the neural network model combined with NDPSO is better than that of LSTM or BiLSTM models. The NDPSO-BiLSTM model has the highest prediction accuracy of 96.78% in the experiment.

D. Safety Situation Prediction Experiment Results

This paper uses the trained NDPSO-BiLSTM model to carry out a 16-hour safety situation prediction experiment, respectively predict the future safety situation of 5min, 10min, and 15min, and compare the predicted value with the real value. The experimental results are shown in Fig. 3 to Fig. 5.

The MAPE values of the three prediction results are 5.53%, 6.31%, and 6.47% in sequence. If the error is regarded as a normal distribution, the standard deviation of the three error normal distributions can be calculated as 6.67%, 7.84%, and 8.04%, and the confidence interval can be calculated as shown in TABLE II.

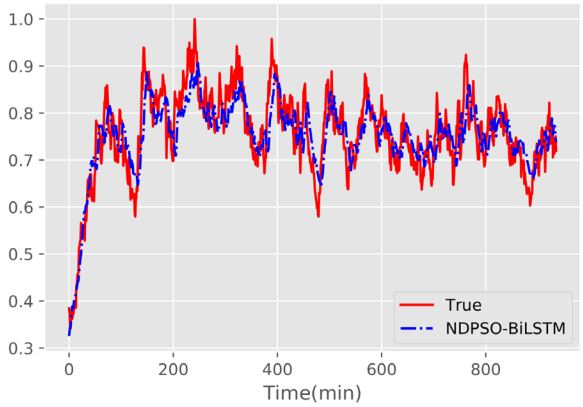

Fig. 3. Forecast results for the next 5 minutes

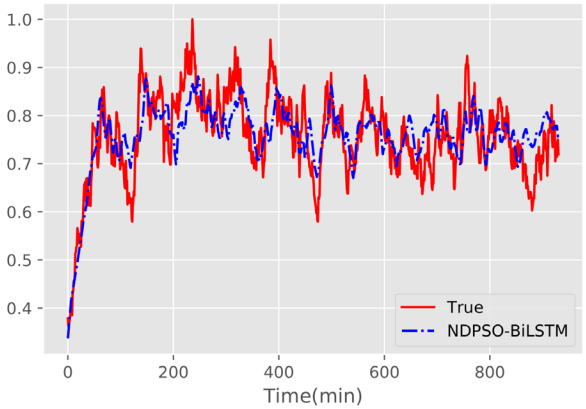

Fig. 4. Forecast results for the next 10 minutes

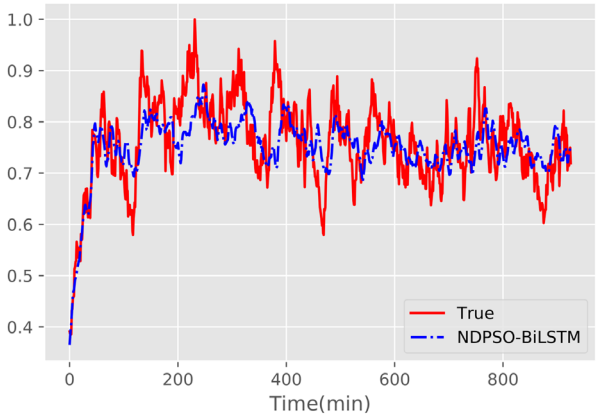

Fig. 5. Forecast results for the next 15 minutes

TABLE II. STATISTICAL TABLE OF CONFIDENCE INTERVALS FOR PREDICTION ERRORS (%）

Forecast duration	95%	90%	80%	70%
5 min	13.07	10.97	8.57	6.90
10 min	15.37	12.90	10.08	8.12
15 min	15.75	13.22	10.33	8.32

It can be seen from TABLE II that in the next 5 minutes of the security situation prediction results, 95% of the prediction data has an absolute error of less than 13.07%. In the next 15 minutes of security situation prediction results, 95% of the data errors are less than 15.75%. Through the above analysis, we proved the feasibility of NDPSO-BiLSTM model for SDN data plane security situation prediction.

V. CONCLUSION

This paper designs a hierarchical security situation assessment method based on the characteristics of software-defined network architecture and the security events in the SDN data plane. Then, the situation assessment results are analyzed, and the correlation in time sequence is tapped. Then a security situation prediction model based on improved particle swarm optimization algorithm and bidirectional long-short-term memory neural network is proposed to realize the security situation prediction for the SDN data plane. The simulation results show that the prediction model has higher prediction accuracy on the test set and is feasible in practical applications.

ACKNOWLEDGMENT

The work of this paper is supported by the project of National Key Research and Development Program of China (No. 2017YFB0801804), "the Fundamental Research Funds for the Central universities" (Grant No. HIT.NSRIF.2020098), Key Research and Development Program of Shandong Province (No.2017CXGC0706).

REFERENCES

[1] N. McKeown, "Software-defined networking," INFOCOM keynote talk, vol. 17, no. 2, pp. 30-32, 2009.

[2] N. McKeown et al., "OpenFlow: enabling innovation in campus networks," ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, 2008.

[3] D. Zhao and J. Liu, "Study on network security situation awareness based on particle swarm optimization algorithm," Computers & Industrial Engineering, vol. 125, pp. 764-775, 2018.

[4] Y. Chen, X. Yin, and A. Sun, "Network Security Situation Assessment Model Based on GSA-SVM," DEStech Transactions on Computer Science and Engineering, no. CCNT, pp. 414-420, 2018.

[5] Y. Jin, Y. Shen, G. Zhang, and H. Zhi, "The model of network security situation assessment based on random forest," in 2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2016: IEEE, pp. 977-980.

[6] Z. Zhan, M. Xu, and S. Xu, "Predicting Cyber Attack Rates With Extreme Values," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1666-1677, 08/01 2015.

[7] A. Okutan, G. Werner, K. McConky, and S. Yang, POSTER: Cyber Attack Prediction of Threats from Unconventional Resources (CAPTURE). 2017, pp. 2563-2565.

[8] S. Chen, Y. Han, D. H. Chau, C. Gates, M. Hart, and K. Roundy, "Predicting Cyber Threats with Virtual Security Products," in annual computer security applications conference, 2017, pp. 189-199.

[9] W. Zhao, H. Yang, J. Li, L. Shang, L. Hu, and Q. Fu, "Network Traffic Prediction in Network Security Based on EMD and LSTM," in Proceedings of the 9th International Conference on Computer Engineering and Networks(CENet), 2019, pp. 461-469.

[10] G. Yang, Q. M. Jie, and N. Q. Tao, "Prediction of ship motion attitude based on BP network," in 2017 29th Chinese Control And Decision Conference (CCDC), 2017, pp. 1596-1600.

[11] G. Zhang, F. Tan, and Y. Wu, "Ship Motion Attitude Prediction Based on an Adaptive Dynamic Particle Swarm Optimization Algorithm and Bidirectional LSTM Neural Network," IEEE Access, vol. 8, pp. 90087-90098, 2020.

[12] J. Kennedy and R. Eberhart, "Particle swarm optimization," in Proceedings of ICNN'95 - International Conference on Neural Networks, 1995, vol. 4, pp. 1942-1948.

[13] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: rapid prototyping for software-defined networks," in Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, 2010: ACM, p. 19.

[14] P. Berde et al., "ONOS: towards an open, distributed SDN OS," in Proceedings of the third workshop on Hot topics in software defined networking, 2014: ACM, pp. 1-6.

[15] T. Benson, A. Akella, and D. A. Maltz, "Network traffic characteristics of data centers in the wild," in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, 2010: ACM, pp. 267-280.

[16] S. Avallone, S. Guadagno, D. Emma, A. Pescapè, and G. Ventre, "D-ITG distributed internet traffic generator," in First International Conference on the Quantitative Evaluation of Systems, 2004: IEEE, pp. 316-317.

[17] Scapy. https://scapy.net/.

[18] G. H. Rosa, J. P. Papa (2019). Soft-Tempering Deep Belief Networks Parameters Through Genetic Programming. Journal of Artificial Intelligence and Systems, 1, 43–59.